The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/27/2009

SUBJECT:
Multiple Vulnerabilities Discovered within IBM WebSphere Application Server

OVERVIEW:
Multiple vulnerabilities have been discovered in the IBM WebSphere Application Server (WAS). IBM WebSphere Application Server (WAS) is a widely used server solution designed for delivering web-based applications and services over the Internet. WAS can be implemented on many common operating systems. These vulnerabilities may allow attackers to bypass authentication, cause denial-of-service or disclose sensitive information. Successful exploitation may allow malicious users to gain unauthorized access to the system, which may lead to other attacks.

SYSTEMS AFFECTED:

- IBM WebSphere Application Server 6.1.0
- IBM WebSphere Application Server 6.1.0 .1
- IBM WebSphere Application Server 6.1.0 .14
- IBM WebSphere Application Server 6.1.0 .2
- IBM WebSphere Application Server 6.1.0 10
- IBM WebSphere Application Server 6.1.0 12
- IBM WebSphere Application Server 6.1.0 13
- IBM WebSphere Application Server 6.1.0 15
- IBM WebSphere Application Server 6.1.0 17
- IBM WebSphere Application Server 6.1.0 18
- IBM WebSphere Application Server 6.1.0 19
- IBM WebSphere Application Server 6.1.0 20
- IBM WebSphere Application Server 6.1.0 21
- IBM WebSphere Application Server 6.1.0 22
- IBM WebSphere Application Server 6.1.0 23
- IBM WebSphere Application Server 7.0
- IBM WebSphere Application Server 7.0.0 1
- IBM WebSphere Application Server 7.0.0 3
- IBM WebSphere Application Server SCA 1.0

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:
IBM has confirmed the existence of multiple vulnerabilities that may allow a remote attacker to bypass application server authentication. Exploiting these vulnerabilities could allow an attacker to access restricted services, which may then lead to other attacks.

IBM WebSphere Application Server 'wsadmin' Security Bypass Vulnerability
IBM WebSphere Application Server is prone to a security bypass vulnerability that affects the 'wsadmin' tool in the System Management/Repository component. Successful exploitation may allow attackers to bypass Java Management Extensions Management Beans (MBeans) security restrictions to stop the server. This would allow an attacker to conduct further attacks.

IBM WebSphere Application Server Weak Password Obfuscation Denial of Service Vulnerability
A vulnerability exists in the way that IBM WebSphere Application Server stores a weak password in the 'ibm-webservicesclient-bind.xml' file. Successful exploitation of this vulnerability may lead to a denial of service condition. Local access to the server is required for this vulnerability to be exploited.

IBM WebSphere Application Server 'ibm-portlet-ext.xmi' Security Bypass Vulnerability
A vulnerability has been discovered in the way that IBM WebSphere Application Server properly reads the 'portlet serving enable' parameter from the 'ibm-portlet-ext.xmi' file. Successful exploitation may allow attackers to bypass certain security restrictions, which may then lead to other attacks.

IBM WebSphere Application Server Migration Component Trace Information Disclosure Vulnerability
An information-disclosure vulnerability exists in IBM WebSphere Application Server when tracing is enabled during a migration between WebSphere Application Server 6.1 and 7.0. Successful exploitation of this vulnerability may allow attackers to preview the trace file and obtain sensitive information.

IBM WebSphere Application Server for z/OS File Permission Vulnerability
IBM WebSphere Application Server is prone to a file permission vulnerability. This issue arises when the WebSphere Application Server fails to securely set permissions on files that were

created during application deployment. Successful exploitation may allow attackers to attempt further attacks. Local access to the server is required for this vulnerability to be exploited.

IBM WebSphere Application Server Single Sign On Security Bypass Vulnerability
IBM WebSphere Application Server is prone to a vulnerability that is caused by a design error found within Single Sign-on and is configured with the SPNEGO implementation. This vulnerability may be exploited when the custom property 'ws.webcontainer.invokefilterscompatibility' is set to true, which allows attackers to bypass Single Sign-on authentication on secure URLs. Successful exploitation may lead to further attacks.

IBM WebSphere Application Server SCA Security Bypass Vulnerability
A vulnerability exists in the Service Component Architecture (SCA) feature pack of IBM WebSphere Application Server. Attackers that could create or obtain access to an account that has not been assigned to the 'scaAllAuthorizedUsers' role could exploit this issue to gain unauthorized access. Successful exploitation may allow attackers to bypass 'authentication.transport' security restrictions, which may then lead to other attacks.

IBM WebSphere Application Server 'CSIv2' Security Bypass Vulnerability
A security bypass vulnerability has been discovered in IBM WebSphere Application Server. This issue arises in the way that the WebSphere Application Server handles an unspecified error when the CSIv2 Security parameter is configured with the Identity Assertion. Exploiting this issue can occur through attack vectors related to Enterprise Java Beans. Successful exploitation may allow a malicious user to conduct further attacks.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by IBM to vulnerable systems immediately after appropriate testing.
- Apply the principle of Least Privilege to all services.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/36153
http://www.securityfocus.com/bid/36154
http://www.securityfocus.com/bid/36155
http://www.securityfocus.com/bid/36156
http://www.securityfocus.com/bid/36157
http://www.securityfocus.com/bid/36158
http://www.securityfocus.com/bid/36159
http://www.securityfocus.com/bid/36163

Secunia:

http://secunia.com/advisories/36306/

IBM:
http://www-01.ibm.com/support/docview.wss?uid=swg27014463
http://www-01.ibm.com/support/docview.wss?uid=swg27007951
http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27004980

ISS X-Force:
http://xforce.iss.net/xforce/xfdb/52074
http://xforce.iss.net/xforce/xfdb/52076
http://xforce.iss.net/xforce/xfdb/52079
http://xforce.iss.net/xforce/xfdb/52081
http://xforce.iss.net/xforce/xfdb/52082
http://xforce.iss.net/xforce/xfdb/52083
http://xforce.iss.net/xforce/xfdb/52375

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2090
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2092
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2089
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2091
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2088
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0906

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2085